

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

JOSEPH MESSINA, CLINT SCOLES, and
CLIFTON DIAZ on Behalf of Themselves and
All Others Similarly Situated,

Plaintiffs,

v.

BASEBALL AMERICA INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Joseph Messina, Clint Scoles, and Clifton Diaz (“Plaintiffs”), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against Defendant Baseball America Inc. (“Baseball America” or “Defendant”) which owns and manages a video streaming service at <https://www.baseballamerica.com/> (the “Website”). On the Website, Defendant utilized tracking tools to intercept and disclose consumers’ search terms, video watching information, and personally identifiable information (collectively, “Sensitive Information”) without seeking or obtaining consumers’ consent (the “Tracking Tools”). Defendant’s use of Tracking Tools resulted in violations of the Video Privacy Protection Act (“VPPA”), federal and state wiretap laws, and invasions into consumers’ privacy. Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who subscribed to Defendant’s Website and subsequently watched pre-recorded video materials (the “Subscribers”).

2. Defendant is a media company specializing in baseball coverage. The publication currently operates across multiple platforms: an editorial and statistics website, a monthly magazine, a podcast network, and three annual reference book titles.

3. Baseball America offers three subscription plans: a monthly digital subscription for \$24.95 per month to gain access to all of Baseball America's digital content; an Annual Digital Subscription at \$99.99 per year for full access to Baseball America's digital content; and a Bundle Plan for \$159.99 per year combining digital access with a year of Baseball America's magazine.¹ Consumers can also sign up to receive newsletters and product updates by providing their personal information.²

4. As a subscriber to any one of Baseball America's three plans or its newsletter, Baseball America provides pre-recorded video content as part of its offerings to subscribers on the Website. These videos include in depth analyses, discussions about baseball prospects, and other related topics. Accordingly, Defendant is in the business of providing pre-recorded videos to Subscribers.

5. Defendant integrates pieces of code referred to as Tracking Tools on its webpages that contain pre-recorded video content. When the webpage or video is accessed, the user's browser loads the Tracking Tools, allowing third parties to collect various types of data about the user such as the IP address (revealing location and ISP), time of access, and the user's activity on the webpage, including the title of the pre-recorded video content they watch.

6. Defendant's decision to place the Tracking Tools on each webpage containing its video materials on the Website ensures that third parties monitor all instances of searching and streaming Defendant's videos.

¹ *Subscribe to Baseball America, Subscription Plans*, BASEBALL AMERICA, <https://www.baseballamerica.com/sign-up/> (last visited Apr. 15, 2025)

² *Join The Newsletter*, BASEBALL AMERICA, <https://www.baseballamerica.com/join-the-newsletter/> (last visited Apr. 15, 2025)

7. Defendant does not disclose to Subscribers that their Sensitive Information, including their protected PII,³ video watching information, and precise webpage information, would be captured by the Tracking Tools, and then transmitted to third parties.

8. Defendant does not inform Subscribers that their Sensitive Information will be exposed, available, and readily usable by any person of ordinary technical skill who receives that data.

9. At no point during or after the account sign up process does Defendant seek or obtain consent for the sharing of Subscribers' Sensitive Information, which Defendant surreptitiously gathered using the Tracking Tools that it chose to employ on the Website. Assuming Defendant's Terms of Use had been presented to Subscribers,⁴ the Terms still do not warn Subscribers that their Sensitive Information will be disclosed to Facebook.

Video Privacy Violations

10. In today's data driven world, a company's data sharing policies for a service or subscription are important factors for individuals to consider in deciding whether to provide personal information to that service or commit to a subscription.

11. Congress has recognized the immediate and irreversible harm caused by associating and disclosing a person's personally identifiable information in conjunction with their video watching information.

³ 18 U.S.C. § 2710(a)(3) ("includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider").

⁴ Defendant's Terms are hyperlinked under the "Sign Up" button on the sign-up page, accompanied by the following text: "By clicking below, you're agreeing . . ." This "sign-in wrap" agreement does not sufficiently put consumers on notice of the agreement. *Morrison v. Yippee Ent. Inc.*, No. 24-CV-0797-MMA-KSC, 2024 WL 4647296, at *13 (S.D. Cal. Oct. 31, 2024) (denying Defendant's motion to compel arbitration).

12. Congress' enactment of the VPPA, and its continued endorsement of the statute, supports that recognition. The VPPA prohibits video tape service providers ("VTSP"),⁵ such as Defendant, from sharing consumers' PII without valid consent.⁶

13. Congress made clear that the harm to individuals impacted by VPPA violations occurs the moment, and each time, a subscriber's information is shared.

14. On the Website, because of Defendant's decision to employ Meta Platform, Inc.'s ("Meta" or "Facebook") tracking pixel (the "Pixel") on the Website, a Subscriber's Sensitive Information is shared *the moment* the Subscriber requests video materials.⁷

15. Defendant purposefully implemented and utilized the Pixel, which tracks Subscribers' activity on the Website and discloses that information to Facebook to gather valuable marketing data. The Pixel could not be placed on the Website without steps taken directly by or on behalf of Defendant (*see* Section B(1)).

16. To be clear, the Pixel cannot be placed on a website by Facebook. Only a website owner can place the Pixel on a website. Here, the Pixel was utilized on the Website and effectuates the sharing of Subscribers' PII. None of this could have occurred without purposeful action on the part of Defendant.

⁵ VTSP refers to "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials" 18 U.S.C. § 2710(a)(4).

⁶ 18 U.S.C. § 2710(b)(2)(B)(i)-(iii).

⁷ As defined by the VPPA, protected "personally identifiable information" includes information which identifies a person as having "requested or obtained" video materials. See 18 U.S.C. § 2710(a)(3). When a website user clicks a link leading to a video, the user "requests" authorization to access the material from the website's server and, if authorized, the server then sends the data to the user. See *How the web works*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited Apr. 15, 2025).

17. Defendant does not seek and has not obtained consent from Subscribers to utilize the Pixel to track, share, and exchange their Sensitive Information with Facebook.

18. When a party, such as Defendant, utilizes the Pixel, it is provided with details about its functionality, including the collection and disclosure of its Subscribers' Sensitive Information.⁸

19. In fact, it is made aware that one of the functions of the Pixel is to collect and share Sensitive Information to “use that information to provide measurement services [] [and] target and deliver ads.”⁹

20. Facebook also advises and directs website owners that there are notice and consent requirements associated with the use of the Pixel and that website owners are responsible for providing that notice and obtain those consents.

21. Not only did Defendant know that Subscribers' Sensitive Information would be shared, but it was also on notice of its obligations to provide notice of its data gathering practices and obtain consent from Subscribers.

22. Defendant cannot claim surprise as to the nature of the Pixel when Facebook itself warned websites utilizing the Pixel, aside from needing “a clear and prominent notice on each web page where [its] Pixels are used[,]” that they must “ensure, in a verifiable manner, that an end user provide[d] all necessary consents before [Augustine Institute] use[d] [Facebook’s Pixel] to enable the storage of and access to Meta cookies . . . [i]n jurisdictions that require informed

⁸ See, e.g., *Meta Business Tools Terms*, FACEBOOK (Apr. 25, 2023), <https://www.facebook.com/legal/terms/businessstools> (“You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage . . . Meta[] may use cookies web beacons and other storage technologies to collect or receive information from your websites”) (last visited Apr. 15, 2025).

⁹ *Id.*

consent.”¹⁰ Employing the Pixel on the Website caused Subscribers’ PII to be shared with Facebook, resulting in VPPA violations.

23. Defendant, despite its use of the Pixel on the pages of the Website containing pre-recorded video content, failed to obtain Subscribers’ consent to allow the Pixel to operate in a way that shares Subscribers’ Sensitive Information with Facebook.

Wiretap Violations

24. Federal and state legislatures addressed citizens’ privacy expectations when communicating with parties via electronic communications.

25. Congress passed the Federal Wiretap Act, which prohibits the unauthorized interception of electronic communications.

26. Pennsylvania’s Wiretapping and Electronic Surveillance Control Act (“WESCA”), 18 Pa. C.S. § 5701 *et seq.* “prohibits the interception of wire, electronic, or oral communications, which means it is unlawful to acquire those communications using a device.”¹¹

27. Defendant purposefully implemented and utilized the Tracking Tools to intercept and read Subscribers’ communications with the Website. Defendant knew that the Tracking Tools would feed Subscribers’ communications to Facebook. The Website does not provide notice of or obtain consent as to such practices.

28. Subscribers of the Website have been harmed because of Defendant’s violations of the VPPA, the Federal Wiretap Act, and WESCA. In addition to monetary damages, Plaintiffs

¹⁰ *Id.*; see *infra* Section B(4).

¹¹ *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121, 124 (3d Cir. 2022).

seek injunctive relief requiring Defendant to immediately (i) remove the Tracking Tools from the Website, or (ii) add adequate notices and obtain the appropriate consent from Subscribers.¹²

29. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of subscribers of the Website for violations of the VPPA, 18 U.S.C. § 2710; the Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e); and WESCA, 18 Pa. C.S. § 5701, *et seq.*

PARTIES

30. Plaintiff Joseph Messina is, and has been at all relevant times, a citizen of Pennsylvania who resides in Philadelphia, Pennsylvania. Plaintiff Messina used Defendant's Website to access video content, especially player highlights, through his paid subscription. By interacting with Defendant's Website, Plaintiff Messina's Sensitive Information was disclosed to third parties, including Meta, through Defendant's placement of Tracking Tools, including the Pixel, on the webpages he visited on Defendant's Website. These webpages include but are not limited to the webpages for the search engine, the specific videos he watched, and the webpage through which Plaintiff Messina subscribed to the Website. The Sensitive Information disclosed to third parties included but is not limited to Plaintiff Messina's search terms, the titles or descriptions of videos he watched, and his unique Facebook ID. Plaintiff Messina had an active Facebook account at the time of his interactions with Defendant's Website. Shortly after visiting

¹² Website owners like Defendant also have the option to anonymize the video's title within the URL or encrypt the video title using hashing, as described by Facebook. *See Advanced Matching, Meta*, <https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching#security> (last visited Apr. 15, 2025); *Meta Business Tools Terms, Facebook* (Apr. 25, 2023), <https://www.facebook.com/legal/terms/businessstools> (last visited Apr. 15, 2025) ("When using a Meta image pixel or other Meta Business Tools, you or your service provider must hash [personally identifiable information] in a manner specified by us before transmission.").

the Website to view video content, Plaintiff Messina began to receive unsolicited advertisements relating to the videos he watched. Plaintiff Messina saw nothing on the Website that suggested to him that his Sensitive Information would be disclosed to unauthorized third parties and did not authorize, consent to, or otherwise engage or permit the disclosure of his Sensitive Information to Meta or any third party. Plaintiff Messina would not have used the Website to access video content had he known that his Sensitive Information would be disclosed to unauthorized third parties.

31. Plaintiff Clint Scoles is, and has been at all relevant times, a citizen of Nebraska who resides in Omaha, Nebraska. Plaintiff Scoles used Defendant's Website to access video content, especially videos about international prospects and draft prospects, through his paid subscription. By interacting with Defendant's Website, Plaintiff Scoles's Sensitive Information was disclosed to third parties, including Meta, through Defendant's placement of Tracking Tools, including the Pixel, on the webpages he visited on Defendant's Website. These webpages include but are not limited to the webpages for the search engine, the specific videos he watched, and the webpage through which Plaintiff Scoles subscribed to the Website. The Sensitive Information disclosed to third parties included but is not limited to Plaintiff Scoles's search terms, the titles or descriptions of videos he watched, and his unique Facebook ID. Plaintiff Scoles had an active Facebook account at the time of his interactions with Defendant's Website. Shortly after visiting the Website to view video content, Plaintiff Scoles began to receive unsolicited advertisements relating to the videos he watched. Plaintiff Scoles saw nothing on the Website that suggested to him that his Sensitive Information would be disclosed to unauthorized third parties and did not authorize, consent to, or otherwise engage or permit the disclosure of his Sensitive Information to Meta or any third party. Plaintiff Scoles would not have used the Website to access video content had he known that his Sensitive Information would be disclosed to unauthorized third parties.

32. Plaintiff Clifton Diaz is, and has been at all relevant times, a citizen of West Virginia who resides in Morgantown, West Virginia. Plaintiff Diaz used Defendant's Website to access video content, especially videos about prospects and training camp, through his paid subscription. By interacting with Defendant's Website, Plaintiff Diaz's Sensitive Information was disclosed to third parties, including Meta, through Defendant's placement of Tracking Tools, including the Pixel, on the webpages he visited on Defendant's Website. These webpages include but are not limited to the webpages for the search engine, the specific videos he watched, and the webpage through which Plaintiff Diaz subscribed to the Website. The Sensitive Information disclosed to third parties included but is not limited to Plaintiff Diaz's search terms, the titles or descriptions of videos he watched, and his unique Facebook ID. Plaintiff Diaz had an active Facebook account at the time of his interactions with Defendant's Website. Shortly after visiting the Website to view video content, Plaintiff Diaz began to receive unsolicited advertisements relating to the videos he watched. Plaintiff Diaz saw nothing on the Website that suggested to him that his Sensitive Information would be disclosed to unauthorized third parties and did not authorize, consent to, or otherwise engage or permit the disclosure of his Sensitive Information to Meta or any third party. Plaintiff Diaz would not have used the Website to access video content had he known that his Sensitive Information would be disclosed to unauthorized third parties.

33. Defendant Baseball America Inc., headquartered in Durham, North Carolina is a sports publication company that covers baseball. It is currently published in the form of an editorial and stats website, a monthly magazine, a podcast network, and three annual reference book titles. It also regularly produces lists of the top prospects in the sport, and covers aspects of the game from a scouting and player development point of view.

JURISDICTION AND VENUE

34. The District Court for the Middle District of North Carolina has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members; the aggregate amount in controversy exceeds \$5,000,000.00, exclusive of interest, fees, and costs; and at least one Class Member is a citizen of a state different from Defendant. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the Video Privacy Protection Act, 18 U.S.C. § 2710, as well as the Federal Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e).

35. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in North Carolina, and Defendant derives revenue in the State of North Carolina, including Defendant's revenue generated from its management over and sales through the Website, including the revenue sharing, advertising sales, etc. that Defendant derives from the Website.

36. Venue is proper in the Middle District of North Carolina pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and Defendant conducts substantial business operations in this District. In connection with the Website, the subscription sales, and associated coding, all claims originate and arise out of the Defendant's business operations in this District.

COMMON FACTUAL ALLEGATIONS

A. Legislative Background

1. The Video Privacy Protection Act

37. Congress enacted the VPPA in 1988 in response to a Washington, D.C. newspaper's profile of then-Supreme Court nominee Judge Robert H. Bork during his confirmation hearings. *See* S. Rep. No. 100-599, 2d Sess., at 5 (1988). The profile contained a

list of 146 films Judge Bork and his family rented from a video store, obtained without his knowledge or consent. *Id.* Members of Congress denounced the disclosure as repugnant to the right of privacy. *Id.* at 5-8.

38. Recognizing, as Justice Brandeis had decades earlier, that “subtle and more far reaching means of invading privacy have become available,” *Olmstead v. U.S.*, 277 U.S. 438, 473 (1928), Congress passed the VPPA so that individuals can “maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers.” S. Rep. No. 100-599, at 8 (1988).

39. Senator Patrick Leahy explained that the new law was meant to protect “our right to privacy [in] the choice of movies that we watch with our family in our own homes,” as “[t]hese activities are at the core of any definition of personhood.” 134 Cong. Rec. S5397–01, S. 2361 (May 10, 1988).

40. The VPPA prohibits “[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider.” 18 U.S.C. § 2710(b)(1). The VPPA defines personally identifiable information as “information which identifies a person as having requested or obtained specific video materials or services from a video service provider.” 18 U.S.C. § 2710(a)(3). A video tape service provider is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio-visual materials.” 18 U.S.C. § 2710(a)(4). A consumer is “any renter, purchaser, or subscriber of goods or services from a video tape service provider[.]” 18 U.S.C. § 2710(a)(1).

41. The broad language of the definitions contained in the VPPA comports with the initial purpose of the VPPA—to “give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives” by prohibiting “unauthorized disclosures of personal information

held by video tape providers.” S. Rep. No. 100–599, 2d Sess., at 6 (1988).

42. In 2012, Congress amended the VPPA “to reflect the realities of the 21st century.” 158 Cong. Rec. H6849–01 (Dec. 18, 2012).

43. In a Senate Judiciary Committee meeting, Senator Leahy stated, “While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps and other new technologies have revolutionized the availability of Americans’ information.”¹³

44. Senator and Subcommittee Chair Hon. Al Franken stated:

One way we need to update this law is to make sure that it is keeping up with technology. It used to be that if you wanted to watch a video, you had to go to the video store or then wait for it in the mail after that. Now you can stream it directly to your computer in seconds. Streaming is the future of video, . . . it is clear that the law does cover new technologies like streaming because it does not just cover “prerecorded video cassette tapes.” It also covers “similar audio-visual materials.”¹⁴

45. Courts across the country have affirmed a broad reading of the VPPA and its application to modern video sources, such as websites.¹⁵

¹³ See *Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY COMMITTEE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW, available at https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited Apr. 15, 2024).

¹⁴ *Id.*

¹⁵ See, e.g., *Mata v. Zillo Grp., Inc.*, 2024 U.S. Dist. LEXIS 229061, at *8-9 (S.D. Cal. Dec. 18, 2024) (VPPA applied to real estate marketplace website); *Fan v. NBA Properties, Inc.*, 2024 WL 1297643, at *3 (N.D. Cal. Mar. 26, 2024) (holding NFT digital platform is a VTSP subject to the VPPA); *Aldana v. GameStop, Inc.*, 2024 WL 708589, at *3 (S.D.N.Y. Feb. 21, 2024) (holding video game seller is a VTSP); *Sellers v. Bleacher Report, Inc.*, 2023 U.S. Dist. LEXIS 131579, at *15-18 (N.D. Cal. July 29, 2023) (VPPA sufficiently applied to sports news website); *Jackson v. Fandom, Inc.*, 2023 U.S. Dist. LEXIS 125531, at *6 (N.D. Cal. July 20, 2023) (VPPA applies to gaming and entertainment website); *Louth v. NFL*, 2022 U.S. Dist. LEXIS 163706, at *11-12 (D.R.I. Sep. 12, 2022) (holding VPPA applied to NFL’s videos accessible through mobile app).

46. Video tape service providers (“VTSPs”) are not required to deal exclusively in audio visual content; rather, audiovisual content need only be part of the provider’s book of business. *Salazar v. Nat’l Basketball Ass’n*, 118 F.4th 533, 547-48 (2d Cir. 2024).

47. The *Salazar* Court also reasoned that “‘consumer’ should be understood to encompass a renter, purchaser, or subscriber of *any* of the provider’s ‘goods or services’—audiovisual or not.” *Salazar*, 118 F.4th at 548-49; *see also Lee v. Springer Nature Am., Inc.*, No. 24-CV-4493 (LJL), 2025 WL 692152, at *8 (S.D.N.Y. Mar. 4, 2025).

48. The VPPA prohibits the disclosure of PII, including “information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior.” *In re Nickelodean Consumer Priv. Litig.*, 827 F.3d 262, 267 (3d Cir. 2016). For example, “[a] Facebook link or an email address may very well readily enable an ‘ordinary person’ to identify an individual.” *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 986 (9th Cir. 2017).

49. Defendant here is a VTSP in that they provided pre-recorded audio-visual materials to Plaintiffs and Class Members through its design and provision of, and continued involvement with the OTT Websites.

50. In this case, Plaintiffs’ VPPA-protected Sensitive Information was knowingly and systematically disclosed to third parties by Defendant, without obtaining Plaintiffs’ consent.

2. The Federal Wiretap Act

51. The Wiretap Act, as amended through the 1986 Electronic Communications Privacy Act (“ECPA”), provides a private right of action for private intrusions as though they were government intrusions.¹⁶

52. In passing the ECPA, Congress was concerned about technological advancements, such as “large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing.”¹⁷

53. As a result, the ECPA primarily focused on two types of computer services which were prominent in the 1980s: (i) electronic communications, such as email between users; and (ii) remote computing services such as cloud storage or third party processing of data and files.¹⁸

54. An ECPA claim requires a showing that a person or entity “(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept to endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.”¹⁹

55. “Interception” is defined as “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”
18 U.S.C. § 2510(4).

56. An “electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a

¹⁶ Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act’s Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022), available at <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj> (last visited Apr. 15, 2025).

¹⁷ Senate Rep. No. 99-541, at 2 (1986).

¹⁸ *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

¹⁹ *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 900 (C.D. Ca. 2024) (quoting 18 U.S.C. §§ 2510 *et seq.*).

wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12).

57. The “paramount objective of the [ECPA] is to protect effectively the privacy of communications.” *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013).

58. The ECPA “protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers.”²⁰

59. Courts consistently hold that to violate the ECPA, an interception must be “contemporaneous” with the communication. *See, e.g., Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457, 460 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877-78 (9th Cir. 2002); *U.S. v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003).

60. The “unauthorized duplication and forwarding of unknowing users’ information” is among the most common methods of impermissible intrusion. *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020).

61. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not “intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. §2511(2)(d).

²⁰ Bureau of Justice Assistance U.S. Department of Justice, *Electronic Communications Privacy Act of 1986 (ECPA)*, 18 U.S.C. §§ 2510-2523, BUREAU OF JUST., <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285> (last visited Apr. 15, 2025).

62. While communicating with Defendant on the Website through their viewing choices, Subscribers had the contents²¹ of their communications with Defendant intercepted by Facebook via the Pixel.

63. Defendant purposefully included the Pixel on the Website to intercept Plaintiffs' communications and redirect them to Facebook to improve the effectiveness of its and Facebook's advertising and marketing.

64. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Defendant to Facebook.

3. The Pennsylvania Wiretapping and Electronic Surveillance Control Act

65. Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S. § 5701 *et seq.* has its roots in the common law right to privacy, which protects citizens' "protectable interest in their private information and . . . the sanctity of their communications."²²

66. WESCA operates in conjunction with and as a supplement to the Federal Wiretap Act, which allows states to "grant greater, but not lesser, protection than that available under federal law."²³ WESCA does so.

67. WESCA prohibits: (1) the intentional interception of wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom to another person; and (3) the intentional use of

²¹ The contents of Plaintiffs' and users' communications include: 1) Plaintiffs' search terms; 2) the location and contents of webpages visited by users; and 3) the PII discussed in Section B(2)-(3).

²² *Petris v. Sportsman's Warehouse, Inc.*, No. 2:23-CV-1867, 2024 WL 2817530 (W.D. Pa. June 3, 2024).

²³ *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121, 124 (3d Cir. 2022).

the contents of any wire, electronic or oral communication, or evidence derived therefrom. 18 Pa. C.S. § 5703(a).

68. “Intercept” is defined as: “Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 19 Pa. C.S. § 5702.

69. WESCA defines electronic communication as: “Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature” *Id.*

70. Under WESCA, a court may award actual damages (but not less than liquidated damages computed at the rate of \$100 a day for each violation of the statute, or \$1,000, whichever is higher), punitive damages, equitable relief, and attorney’s fees.

71. In this case, Plaintiffs’ data—their Sensitive Information—constitutes electronic communications with Defendant.

72. Plaintiffs’ electronic communications with Defendant were intentionally intercepted by Defendant through the Tracking Tools that Defendant employs on the Website.

73. Plaintiffs’ electronic communications were subsequently disclosed to third parties.

74. Defendant used the contents of Plaintiffs’ electronic communications with the Website, intercepted and processed by third parties, to target Plaintiffs with advertising.

75. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Defendant.

76. Defendant acted with the intent to intercept, disclose, and use Plaintiffs’ protected, private information for its economic benefit through the monetization of the information via targeted advertising and other means.

B. The Website and the Facebook Pixel

76. Facebook offers the Pixel to web developers for the purpose of monitoring user interactions on their websites, which can then be shared with Facebook.

77. On the Website, Defendant utilized the Facebook Pixel to intercept and disclose Subscribers' Sensitive Information without seeking or obtaining Subscribers' consent.

1. Defendant Implemented the Facebook Pixel on the Website

78. The Pixel is a marketing tool that can only be added to a webpage by website developers. A website operator must sign up for a business account or link a related Facebook account with its Pixel, and then add code to the website to make use of the Pixel.²⁴

79. The Pixel must be added to each individual page that a website owner wishes to be tracked.²⁵

80. Here, Defendant took steps to add the Pixel to the Website.

81. The Pixel is employed by Defendant to gather, collect, and then share user information with Facebook.²⁶ Receiving this information enables Facebook and the web developers to build valuable personal profiles for users, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.²⁷ The sharing of Subscribers' PII benefits Defendant by improving the effectiveness of advertising targeted at Defendant's

²⁴ *Meta Business Help Center: Set up and install the Meta Pixel*, META, <https://www.facebook.com/business/help/952192354843755?id=1205376682832142> (last visited Apr. 15, 2025).

²⁵ *Get Started*, META, <https://developers.facebook.com/docs/meta-pixel/get-started/> (last visited Apr. 15, 2025) ("To install the Pixel, . . . add its base code . . . on every page where you will be tracking website visitor actions").

²⁶ The Facebook Pixel allows websites to track visitor activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta Pixel*, META, <https://developers.facebook.com/docs/meta-pixel/> (last visited Apr. 15, 2025).

²⁷ *See Meta Pixel*, META, <https://www.facebook.com/business/tools/meta-pixel> (last visited Apr. 15, 2025).

Subscribers. Studies have shown that personalization in digital marketing through targeted and dynamic advertising can boost revenue by 15%.²⁸

82. Website owners and operators can choose to use the Pixel to share both user activity (including video watching activity) and user identity with Facebook. Here, Defendant's Website shares both.

83. The harvested data can improve advertising by pinpointing audience demographics by interests, gender, or location and finding the people who are most likely to take action and view content.²⁹

84. The PII harvested by Defendant provides similar, if not more, data, including the titles of videos, whether through webpage URLs, parameters, or metadata, in addition to their Facebook profile data.

85. The owner or operator of a website holds the decision-making authority over the placement of the Pixel on its site, as well as whether or not any of the data within the Pixel transmission should be "hashed" (a form of encryption).

86. To activate and employ a Facebook Pixel, a website owner must first sign up for a Facebook account, where adding the Pixel to the website owner's "business portfolio" provides the most utility for using the Pixel.³⁰ For instance, business portfolios can: (i) create and utilize more simultaneous Pixels; (ii) manage multiple Facebook Pages, Instagram accounts, ad

²⁸ Wilson Lau, *What is Targeted Advertising?*, ADROLL BLOG (June 30, 2024), <https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Benefits%20of%20Targeted%20Advertising,-1.%20Deliver%20a%20higher> (last visited Apr. 15, 2025).

²⁹ See *Audience ad targeting*, META, <https://www.facebook.com/business/ads/ad-targeting> (last visited Apr. 9, 2025).

³⁰ *How to set up your Meta Pixel with a business portfolio*, META, <https://www.facebook.com/business/help/314143995668266?id=1205376682832142> (last visited Apr. 15, 2025).

accounts, and catalogs from a centralized interface; (iii) access and manage multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees); (iv) post or analyze data analytics collected from Facebook pages or Instagram accounts; (v) run ads businesses across Facebook and Instagram; and (v) create and manage shops across Facebook and Instagram.³¹

87. To add an operational Pixel to a website, the website owner or operator must take several affirmative steps, including naming the Pixel during the creation and setup of the Pixel.³²

88. Once the Pixel is created, the website operator assigns access to the Pixel to specific people for management purposes,³³ and must connect the Pixel to a Facebook Ad account.³⁴

89. After following these steps, a website operator can start capturing and sharing information using the Pixel.

90. A Pixel cannot be placed on a website by Facebook. It must be placed directly by or on behalf of the site owner. Augustine Institute did so.

2. The Pixel as a Tracking Tool

91. Once the Pixel is set and activated, it can begin collecting and sharing user activity data as instructed by the website owner.

³¹ *About business portfolios*, META, <https://www.facebook.com/business/help/486932075688253> (last visited Apr. 15, 2025).

³² *Id.*; see also Ivan Mana, *How to Set Up & Install the Facebook Pixel*, YOUTUBE (Feb. 4, 2022), available at <https://www.youtube.com/watch?v=ynTNS5FAUm8> (last visited Apr. 15, 2025).

³³ *Add People to your Meta Pixel in Meta Business Suite or Business Manager*, META <https://www.facebook.com/business/help/279059996069252?id=2042840805783715> (last visited Apr. 15, 2025).

³⁴ *Add an ad account to a Meta Pixel in Meta Business Manager*, META, <https://www.facebook.com/business/help/622772416185967> (last visited Apr. 15, 2025).

92. When a Facebook user logs onto Facebook, a “c_user” cookie – which contains a user’s non-encrypted Facebook User ID number (“UID”) – is automatically created and stored on the user’s device for up to a year.³⁵

93. This means that for Subscribers to the Website who are also Facebook users, their PII is certain to be shared. Their PII is automatically bundled with their web watching history and disclosed to Facebook when visiting a page with an active Pixel, including the home page.

94. While the process to determine what information is being collected by the Pixel from a user is admittedly complicated, the recipient of the Pixel’s transmissions receives the information in a clear and easy to understand manner.

95. The seemingly complex data, such as the long URLs included in the Pixel’s transmission, is “parsed,” or translated into an easier to read format, such that the information is legible.

96. For example, an embedded URL in a Pixel HTTP Request may look like an indecipherable code, as depicted below:

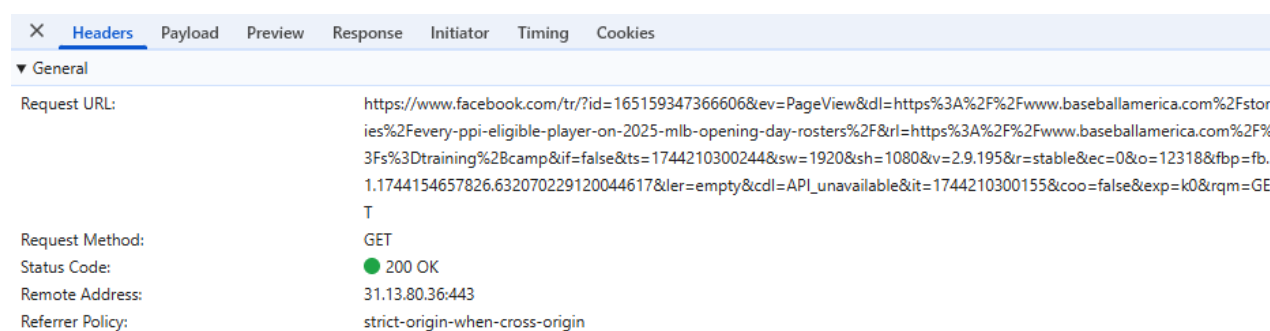


Figure 1 - Sample Pixel Request

³⁵ *Cookies Policy: What are cookies and what does this policy cover?*, META (Dec. 12, 2023), <https://www.facebook.com/policy/cookies/> (last visited Apr. 15, 2025).

97. However, these URLs are designed to be “parsed” into easy-to-digest pieces of information, as depicted below:

X

Headers

Payload

Preview

Response

Initiator

Timing

Cookies

▼ Query String Parameters

view source

view URL-encoded

id: 165159347366606

ev: PageView

dl: https://www.baseballamerica.com/stories/every-pbi-eligible-player-on-2025-mlb-opening-day-rosters/

rl: https://www.baseballamerica.com/?s=training+camp

if: false

ts: 1744210300244

sw: 1920

sh: 1080

v: 2.9.195

r: stable

ec: 0

o: 12318

fbp: fb.1.1744154657826.632070229120044617

ler: empty

cdl: API_unavailable

it: 1744210300155

coo: false

exp: k0

rqm: GET

Figure 2 - Parsed URL Information from Sample Pixel Request

98. Similarly, the cookies attached to the Pixel’s transmissions are parsed, as depicted below:

101. The information contained within the c_user cookie is considered PII. It contains “the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior.”³⁶ Because the Facebook ID number can simply and easily be appended to “www.facebook.com/” to navigate to the relevant user’s profile, it requires no special skill or expertise to identify the user associated with the Facebook ID, and courts have regularly upheld its status as PII.³⁷

102. Any person, even without in-depth technical expertise, can utilize the UID to identify owners of the UID via their Facebook profile. Once the Pixel’s routine exchange of information is complete, the UID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook UID to www.facebook.com (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular UID. Using the UID from *Figure 5*, appending it to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the UID, as depicted below:

³⁶ *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 290 (3d Cir. 2016).

³⁷ *See Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass’n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

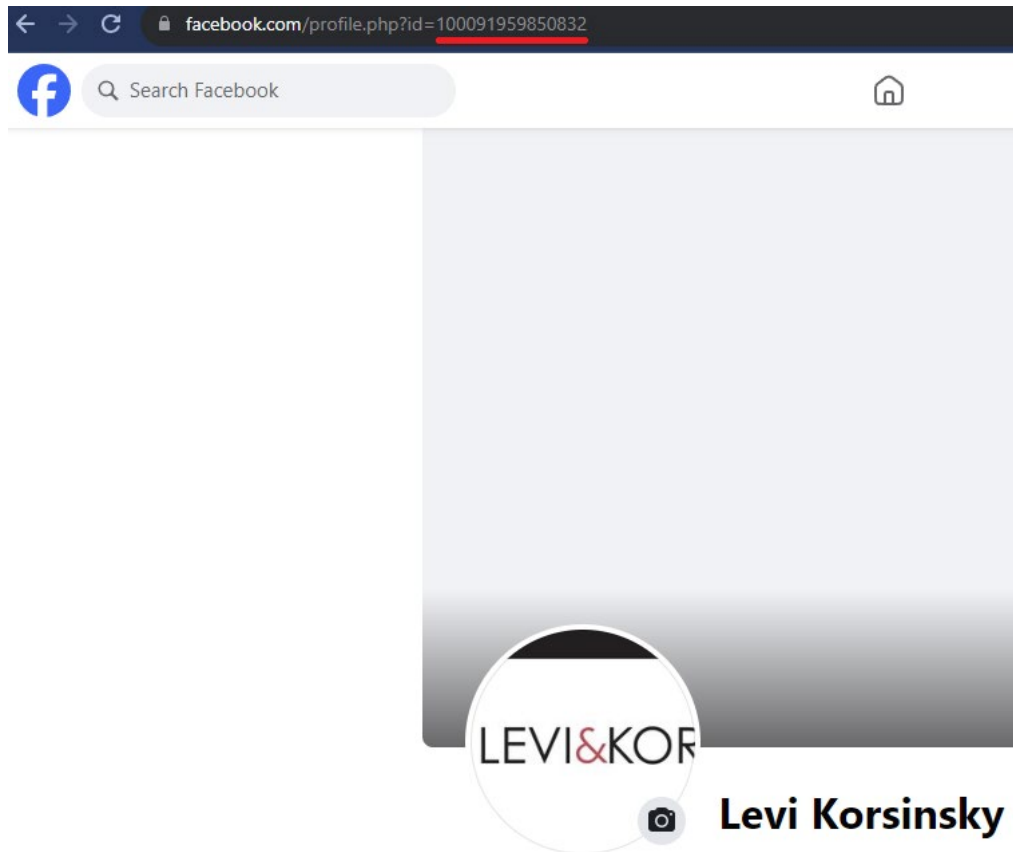


Figure 6 - Result of appending Sample UID of a user to "facebook.com/" being redirected to the user's profile created by Plaintiffs' counsel in a prior investigation into the Pixel

103. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language, and country – are “always public.”³⁸ No privacy setting on Facebook would allow Plaintiffs, or any user, to hide this basic information.

104. By compelling a user's browser to disclose the c_user cookie alongside event data for media content, Defendant knowingly discloses information sufficiently permitting an ordinary person to identify an individual.

³⁸ *Control who can see what you share on Facebook*, FACEBOOK, <https://www.facebook.com/help/1297502253597210> (last visited Apr. 15, 2025).

3. *The Pixel Shares Subscribers' PII*

105. The Pixel tracks user-activity on web pages by monitoring events,³⁹ which when triggered, causes the Pixel to automatically send data – here, Subscribers' PII – directly to Facebook.⁴⁰ Examples of events utilized by websites include: (i) a user loading a page with a Pixel installed (the “PageView event”)⁴¹; and (ii) when pre-designated buttons, like the “Start Free Trial” button, are clicked (the “SubscribedButtonClick” event).⁴² The Website utilizes both.⁴³

106. When the Pixel Events are triggered, a “HTTP Request” is sent to Facebook (through Facebook’s URL www.facebook.com/tr/).⁴⁴ This confirms that the Pixel Events sent data to Facebook. The HTTP Request includes a Request URL and embedded cookies such as the c_user cookie. It may also include information in its Payload,⁴⁵ such as metadata tags. A Request URL, in addition to a domain name and path, contains parameters. Parameters are values added

³⁹ *About* *Meta* *Pixel*, META, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Apr. 15, 2025).

⁴⁰ *See generally id.*

⁴¹ *Specifications for Meta Pixel standard events*, META, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last visited Apr. 15, 2025).

⁴² *Reference: Standard Events*, META, <https://developers.facebook.com/docs/meta-pixel/reference/> (last visited Apr. 15, 2025).

⁴³ The presence of Pixel events, such as the Microdata and PageView events, can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See About the Meta Pixel Helper*, META, <https://www.facebook.com/business/help/198406697184603?id=1205376682832142> (last visited Apr. 15, 2025).

⁴⁴ Surya Mattu et al., *How We Built a Meta Pixel Inspector*, THE MARKUP (Apr. 28, 2022 8:00 AM) <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector> (last visited Apr. 15, 2025).

⁴⁵ The “request payload” (or more simply, “Payload”) is data sent by a HTTP Request, normally through a POST or PUT request, where the HTTP Request has a distinct message body. Payloads typically transmit form data, image data, and programming data. *See Request Payload Variation*, SITESPECT, <https://doc.sitespect.com/knowledge/request-payload-trigger> (last visited Apr. 15, 2025).

to a URL to transmit data and direct a web server to provide additional context-sensitive services, as depicted below:

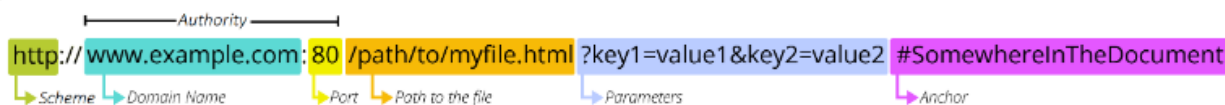


Figure 7 – Mozilla’s diagram of a URL, including parameters⁴⁶

107. Defendant uses the Pixel to collect and share Website Subscribers’ PII with Facebook. Defendant does not disclose its data sharing practices or obtain permission from its Subscribers to share their PII with Facebook.

108. Defendant shares non-anonymized PII with Facebook. Defendant’s disclosures include unique identifiers (the UID) that correspond to specific Facebook users. The recipient finds the PII and web watching history packaged together in a single data transmission which is easily readable by an ordinary person once the PII is packaged and delivered by the Website’s Pixel.

109. Defendant monetizes the Website’s Subscribers by gathering Subscribers’ marketing data and PII and disclosing that valuable information to Facebook. Defendant does so in a format which allows it to make a direct connection between the identity of a Subscriber and that Subscriber’s PII, without the consent of its Subscribers and to the detriment of Plaintiffs’ and Class Members’ legally protected privacy rights.

110. Defendant had and continues to have the choice to design the Website so that the webpage URLs did not include the titles of videos. Defendant had, and has, the choice as to whether to purposefully include more information in the Website’s URLs to improve website

⁴⁶ What is a URL?, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Apr. 15, 2025).

interaction and search engine optimization.⁴⁷ Here, Defendant chose to expose Subscribers' video information so that it could benefit from the tracking and sharing of Subscribers' PII.

111. Defendant also had the power to implement the Pixel in a way that shielded Subscribers' Sensitive Information. Defendant chose, however, to transmit Subscribers' non-anonymized PII.⁴⁸

112. Sensitive data sent to Facebook through the triggered Pixel Events are included within the parameters of the Request URL, within the Request Header, or as a Payload within the request. The specific Pixel Events implemented by Defendant sends Subscribers' PII through the Request URL parameters and HTTP Headers.⁴⁹

113. An "HTTP Header" is a field of an HTTP Request or response that passes additional context and metadata about the request or response.⁵⁰ Specifically, Request Headers are a subset of HTTP Headers that are used to provide information about a request's context, so that a server can customize its response to the request or supply authentication credentials⁵¹ to the server or otherwise provide more information about the client sending the request.⁵²

114. Defendant shares with Facebook the specific films requested by Subscribers to the Website through Request URL parameters.

⁴⁷ See Chima Mmeje, *Different Domain Types and Best Practices for SEO*, MOZ (Nov. 11, 2024) <https://moz.com/learn/seo/domain> (last visited Apr. 15, 2025).

⁴⁸ See *Advanced Matching*, META, <https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching> (last visited Apr. 15, 2025).

⁴⁹ URL parameters are values that are added to a URL to cause a web server to provide additional or different services. *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Apr. 15, 2025).

⁵⁰ *HTTP header*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/HTTP_header (last visited Apr. 15, 2025).

⁵¹ *Id.*

⁵² *Id.*

115. These factual allegations are corroborated by publicly available evidence. For instance, a user visits the Baseball America Website, clicks on a series, such as “Cooper Ingle joins; Andrew Painter added to AFL,” and subsequently watches the film. Defendant’s disclosure of this user’s PII is portrayed in *Figures 8 through 10* below.

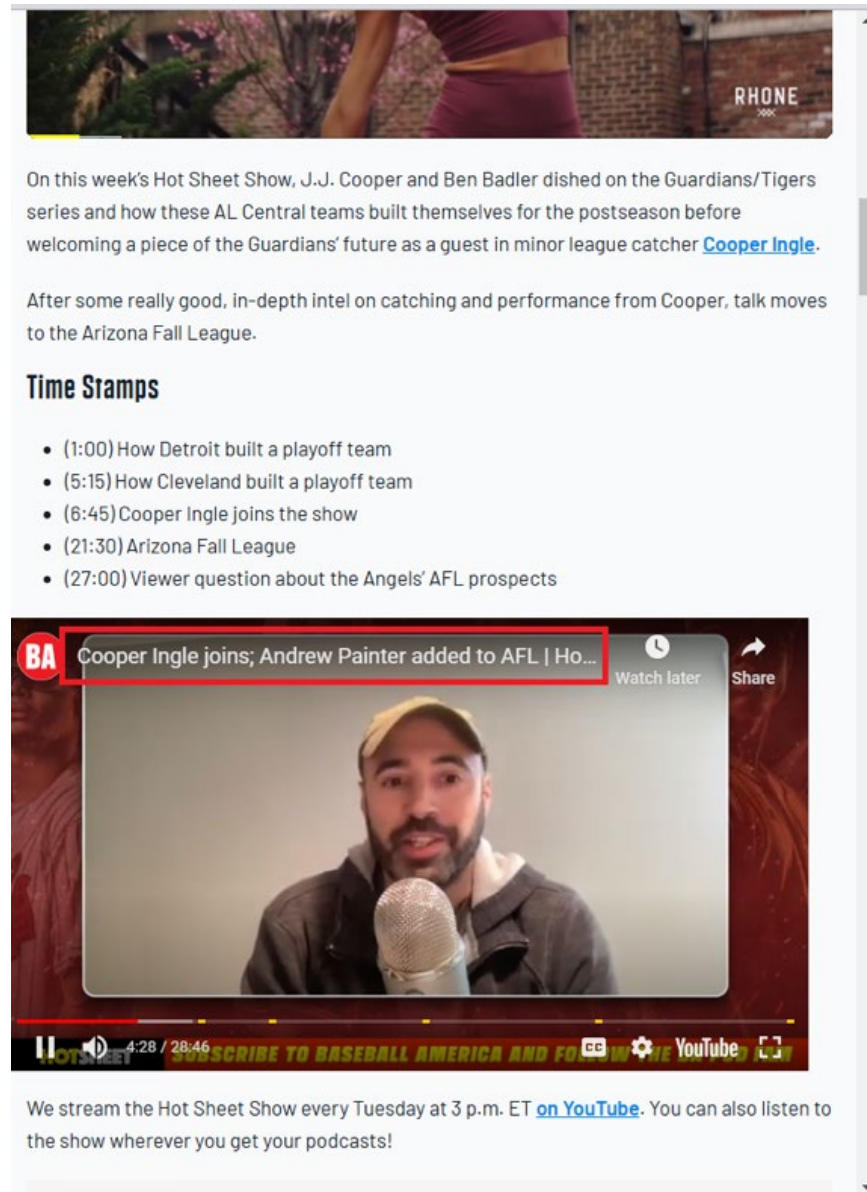


Figure 8 – Sample webpage on the Website with video content

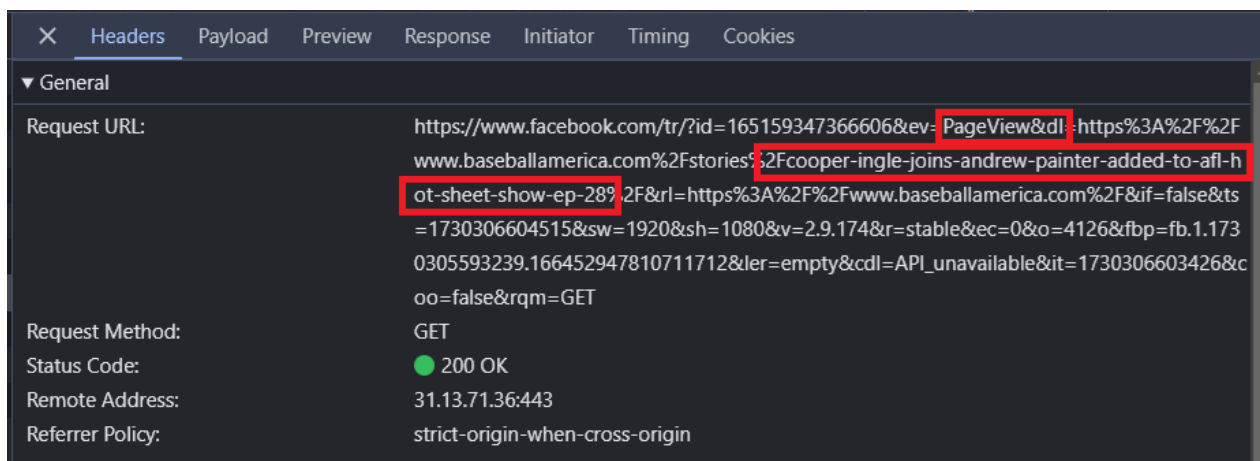


Figure 9 – Video Title included in URL parameters disclosed to Facebook through PageView Pixel Event on the Website

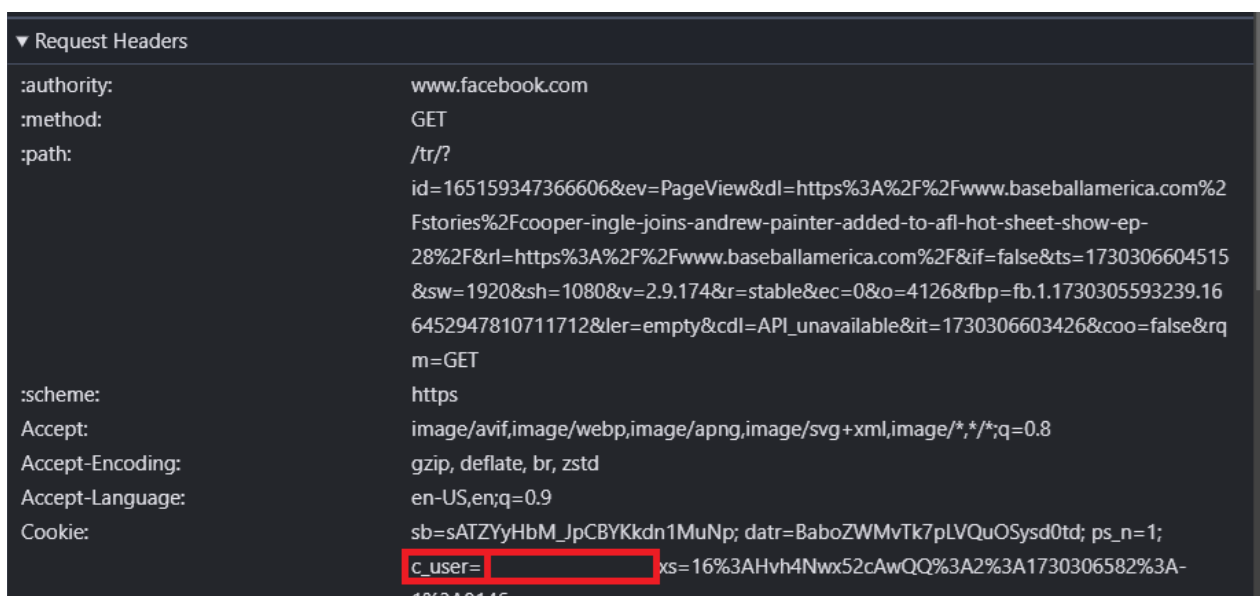


Figure 10 – UID included in URL parameters disclosed to Facebook through PageView Pixel Event on the Website

116. As depicted above in *Figure 10*, Defendant also transmits Subscribers' PII to Facebook in the form of an unencrypted and unique UID contained in the `c_user` cookie included in the HTTP Request Header, which can be used to find a user's personal Facebook page, as discussed in Section B (2) above.

117. The information contained within the `c_user` cookie is considered PII because it contains "the kind of information that would readily permit an ordinary person to identify a specific

individual's video-watching behavior.”⁵³ Because the UID can simply and easily be appended to “www.facebook.com/” to navigate to the relevant user's profile, it requires no special skill or expertise to identify the user associated with the Facebook ID, and courts have regularly upheld its status as PII.⁵⁴

4. Defendant Was Told the Pixel Discloses Subscribers' Data; It Knew Precisely What the Pixel Would Collect and Share

118. When a business applies with Facebook to use the Pixel, it is provided with detail about its functionality (site policy), including with respect to PII.⁵⁵

119. To make use of the Pixel, Defendant agreed to Facebook's Business Tool Terms (the “Business Terms”).

120. The Business Terms informs website owners using Facebook's Pixel that the employment of the Pixel will result in data sharing, including with Facebook, through the automatic sharing of Pixel Event information (“Event Data”) and contact information (“Contact Information”).⁵⁶

⁵³ *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 290 (3d Cir. 2016).

⁵⁴ See *Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass'n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

⁵⁵ See *Get Started*, META, <https://developers.facebook.com/docs/meta-pixel/get-started> (last visited Apr. 15, 2025) (The Pixel “relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can their actions in the Facebook Ads Manager so you can use the data By default, the Pixel will track URLs visited [and] domains visited . . .”).

⁵⁶ *Meta Business Tools Terms*, FACEBOOK (Apr. 25, 2023), https://www.facebook.com/legal/terms/businessstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Apr. 15, 2025).

121. The Business Terms are transparent that Meta will use the Event Data and Contact Information will be processed “solely to match the Contact Information against user IDs (“Matched User IDs”), as well as to combine those user IDs with corresponding Event Data.”⁵⁷

122. Facebook directs parties implementing the Pixel – here, Defendant – to encrypt request information⁵⁸ *before* data can be shared.⁵⁹

123. Facebook further provides Pixel users, such as Defendant, guidance on responsible data handling, and details how data is acquired, used, and stored, including which information is shared with Facebook.

124. Facebook educates or reminds Pixel users of their responsibility to inform their Subscribers of their website’s data sharing, and specifically guides website owners to obtain the requisite rights, permissions, or consents, before sharing information with any third-party.⁶⁰

125. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from use of the Pixel, and ignored Facebook’s warnings to safely handle its Subscribers’ data and to warn its Subscribers that the Website would disclose information in a manner that threatened Subscribers’ VPPA-protected PII.

⁵⁷ *Id.*

⁵⁸ This contrasts with Facebook’s JavaScript Pixel, which automatically encrypts the data being sent. Defendant has specifically chosen the Pixel method which makes users’ information visible. *See id.*

⁵⁹ *Id.*

⁶⁰ *Best practices for privacy and data use for Meta Business Tools*, META, <https://www.facebook.com/business/help/363303621411154?id=818859032317965> (last visited Apr. 15, 2025).

5. The Website Does Not Obtain Subscribers' Informed, Written Consent Pursuant to the VPPA

126. The Website does not seek nor obtain permission from Subscribers, including Plaintiffs and the Class, to share the Subscribers' PII with third parties, including Facebook.

127. The sign-up process for Baseball America does not seek or obtain informed, written consent.

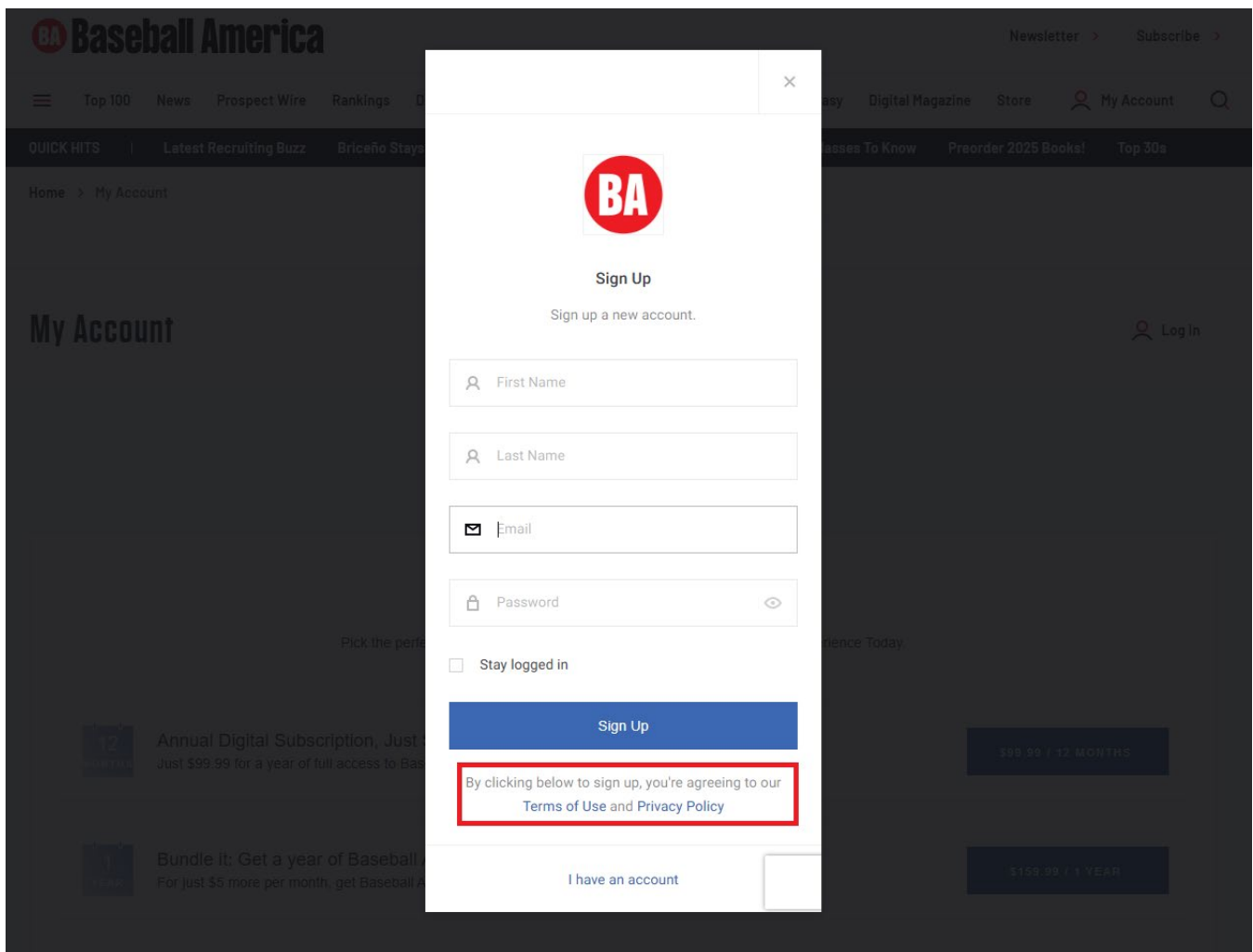


Figure 11 – The Website's Account Registration Webpage

128. To the extent information about any of the Website's data sharing can be located, the language is not (i) presented to consumers of the site in a transparent manner, or where it must be viewed by visitors to the website; and (ii) offered to consumers as checkbox or e-signature

field, or as any form of consent; and (iii) presented in terms that sufficiently warn Subscribers that their information, protected by the VPPA, will be shared with third parties.⁶¹

C. The Google Tracking Tools

129. Google has an array of advertising products, each serving a specific function in advertising portfolios.

1. Google Ads

130. One product, Google Ads (formerly AdWords), is an advertising platform developed by Google, that allows advertisers to place bids to display advertisements, service offerings, product listings, or videos to web users.⁶²

131. The process advertisers using Google Ads to display ads within text-based search results is as follows: (i) advertisers create text-based ads with a title, description, and a link to the website to place within the Google search results; (ii) advertisers then choose keywords, usually related to their business or target audience, intended to trigger their ads to appear within the user's search results;⁶³ (iii) Google then allows advertisers to bid on those various keywords;⁶⁴ (iv) the advertiser with the highest bid wins the auction, and the ad is displayed on the search results page; and (v) the winning ad appears above or below the organic search results and is marked as an ad.

132. Google AdSense, works in conjunction with the Google Ads bidding system, allowing website owners to show Google Ads on websites and earn a revenue share from each ad

⁶¹ See *Privacy Policy*, BASEBALL AMERICA, <https://www.baseballamerica.com/privacy-policy/> (last updated Feb. 13, 2017).

⁶² *Achieve all your goals in one place*, GOOGLE ADS, <https://ads.google.com/home/goals/> (last visited Apr. 15, 2025).

⁶³ *Reach the right people with Search ads*, GOOGLE ADS, <https://ads.google.com/home/campaigns/search-ads/> (last visited Apr. 15, 2025).

⁶⁴ *Id.*

each time it is viewed or clicked on their own sites.⁶⁵ The search terms that various entities bid for through Google Ads are then used by websites owners using Google AdSense to allow website owners to share in the profit Google generates from the advertising.

133. AdSense for content or AdSense for search are methods by which AdSense functions.⁶⁶ In either case, AdSense allows the website host to match ads to the website users based on the website's content and visitors.

134. Google Ads intercepted Plaintiffs' search terms, as depicted, below, using the sample search "Cooper Ingle"

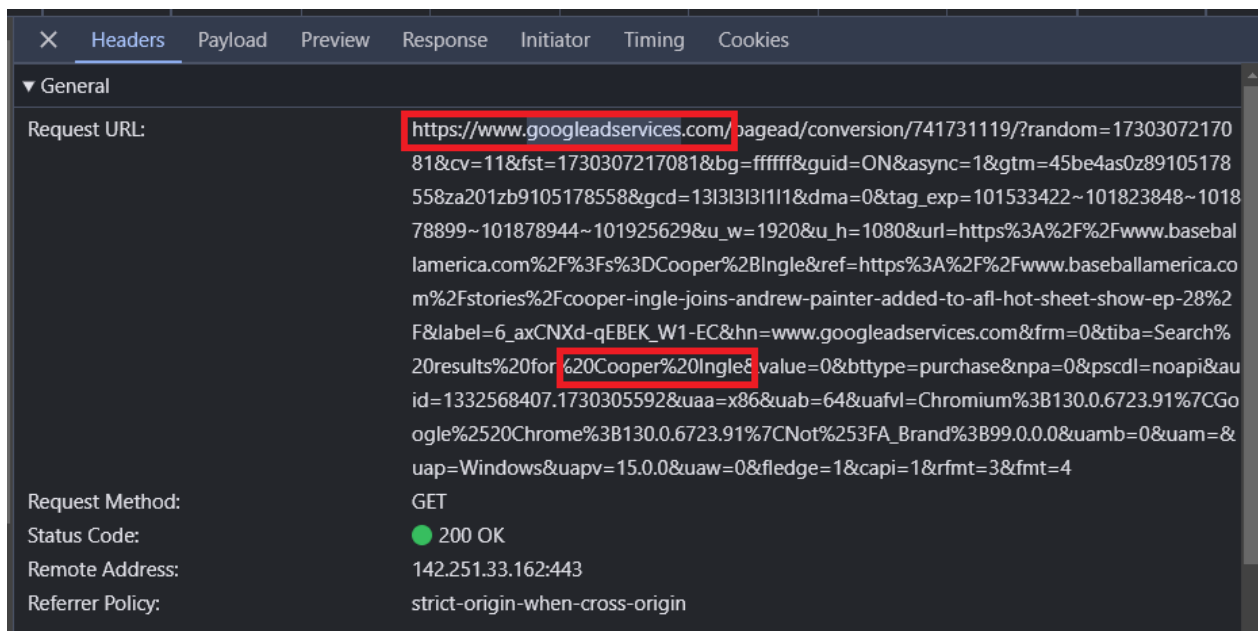


Figure 12 – Test search made on the Website resulted in sharing Search Terms with Google Page Ads

135. Google benefits when website owners utilize Google Ads and Google AdSense in connection with their websites.

⁶⁵ Home, GOOGLE ADSENSE, <https://www.google.com/adsense/start/how-it-works/> (last visited Apr. 15, 2025).

⁶⁶ AdSense revenue share, GOOGLE ADSENSE HELP, <https://support.google.com/adsense/answer/180195?hl=en> (last visited Apr. 15, 2025).

136. Through Google AdSense, Google derives benefits from the ability to aggregate the search data it collects from website users to improve its own services and provide more relevant search results. By understanding patterns and trends in user behavior, Google better understands and gains unencumbered insight into what users are searching for and what they are interested in, which helps Google improve its own services, develop new products and overall increase revenues.

137. Google's collection and analysis of search results also allows it to improve its machine learning algorithms.⁶⁷ Google uses data on how users interact with search results to train its algorithms to provide more accurate and relevant search results.⁶⁸ For example, if a user clicks on a particular search result and spends more time on that page, Google learns that this page is likely more relevant to that search query. By gathering this vast array of data on all users, Google can build an advertising portfolio for each user which includes their gender, age, job industry, and interests.⁶⁹

138. Google profits in several ways from the Website's use of the Google search engine: (i) advertisers bid and pay Google for the keywords that will result in their ads showing in search results; (ii) through AdSense search, every time a user clicks or views an ad (depending on their chosen method), the advertiser will pay Google for that click or view; (iii) and Google's ability to aggregate user search data allows them to further tailor their own products to advertisers and users alike by training its algorithms with vast amounts of search data.

⁶⁷ Elle Poole Sidell, *What Does Google Do With Your Data?*, AVAST (Dec. 18, 2020), <https://www.avast.com/c-how-google-uses-your-data> (last visited Apr. 15, 2025).

⁶⁸ *Id.*

⁶⁹ *Id.*

2. *Google DoubleClick*

139. DoubleClick for Publishers (“DoubleClick”), now also known as Google Ad Manager, allows website owners to monetize their websites by selling ad space within their websites.⁷⁰ DoubleClick connects website owners with advertisers who want to buy ad space within the owners’ website, and allows advertisers to track the performance of their ads across websites.⁷¹ DoubleClick acts as a liaison between a website owner’s ad inventory, relevant ad networks, and advertisers that are looking to purchase ad space on a website.⁷²

140. DoubleClick works in a similar way to Google Ads in that it allows companies to buy impressions through the DoubleClick Ad Exchange.⁷³ DoubleClick is typically used for large-scale advertising as the DoubleClick Ad Exchange connects and aggregates website owners and advertisers of over 100 Ad Exchanges.⁷⁴

141. The process for DoubleClick works as follows: (i) a website operator signs up for the platform by creating a Google Ad Manager account;⁷⁵ (ii) a third-party advertiser then creates an ad campaign using Google AdWords, which includes ad creatives, targeting options, and bid strategies; (iii) the advertiser then submits the ad to DoubleClick where it is reviewed and

⁷⁰ Shubham Grover, *DFP Glossary: An Easier Explanation for All the Jargon*, ADPUSHUP (Dec. 10, 2022), <https://www.adpushup.com/blog/dfp-glossary-easier-explanation-jargon/> (last visited Apr. 15, 2025).

⁷¹ *Id.*

⁷² Brock Munro, *DoubleClick for Publishers: Everything You Need to Know*, PUBLIFT (Dec. 1, 2024), <https://www.publift.com/blog/what-is-googles-dfp-first-look> (last visited Apr. 15, 2025).

⁷³ *DoubleClick Digital Marketing*, GOOGLE, <https://support.google.com/faqs/answer/2727482?hl=en> (last visited Apr. 15, 2025).

⁷⁴ *Id.*

⁷⁵ Munro, *supra* note 68.

approved;⁷⁶ (iv) once approved, the website owner can put the ad on the DoubleClick Ad Exchange to find a buyer for the ad space.⁷⁷

142. Once implemented by the website operator, such as Defendant, when users or Subscribers visit a webpage with a DoubleClick Ad, the user experiences the web page on their browser as an integrated collage of text and images. A DoubleClick Ad, as displayed on the Baseball America Website, is depicted below.

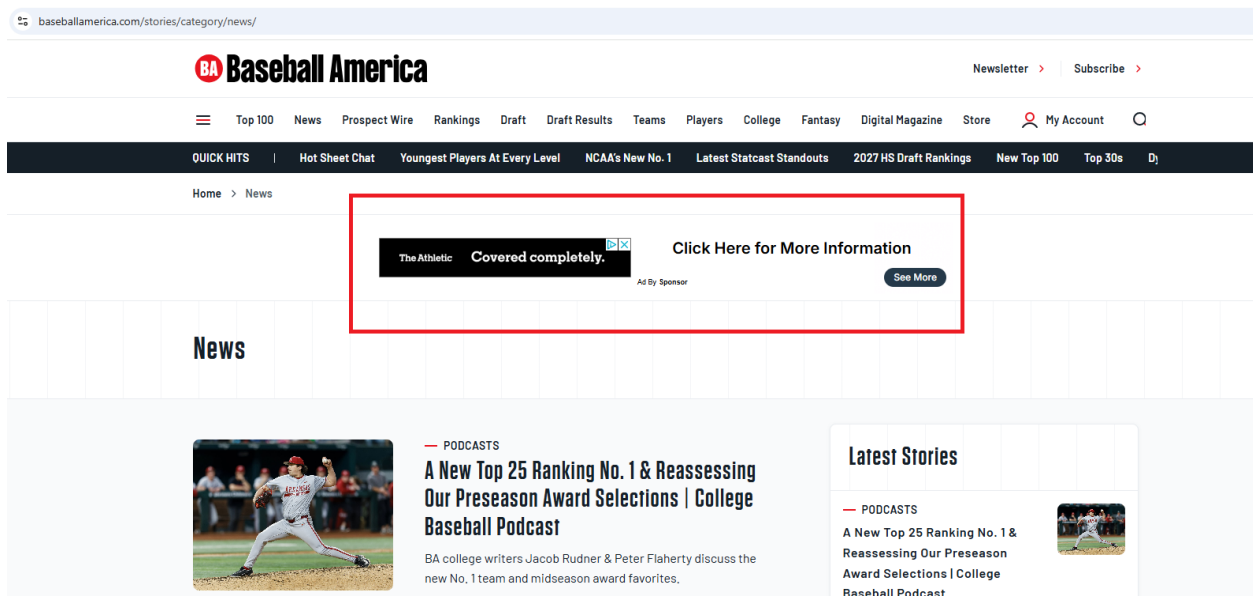


Figure 13 – DoubleClick Ad Banner on Baseball America Website home page

143. However, the content delivered to each webpage is, in reality, aggregated from multiple independent sources. The website owner leaves part of its webpage blank where the third-party advertisements will appear. When a website receives a request from a user visiting a particular webpage, the server for that webpage will respond to the browser, instructing the browser to send a request to the third-party company charged with serving the advertisements for that particular webpage. The third-party's advertising server responds to the user's request by

⁷⁶ See *About the ad review process*, GOOGLE, <https://support.google.com/google-ads/answer/1722120?hl=en> (last visited Apr. 15, 2025).

⁷⁷ Grover, *supra* note 66.

sending the advertisement to the user's browser, which then displays it on the user's device. This entire process occurs within milliseconds and the third-party content appears to arrive simultaneously with the first-party content so that the user does not discern any separate GET requests from the third-parties.

144. Additionally, DoubleClick tracks the performance of ads and provides data such as impressions, clicks, and conversions to the advertiser. That information is then used to further optimize advertising campaigns. The DoubleClick's ad server uses targeting and bidding algorithms to determine which ad to display, based on factors such as the user's location, browsing history, and interest.⁷⁸

145. Defendant sent this information, including users' search terms, to Google via the URL doubleclick.net as depicted below

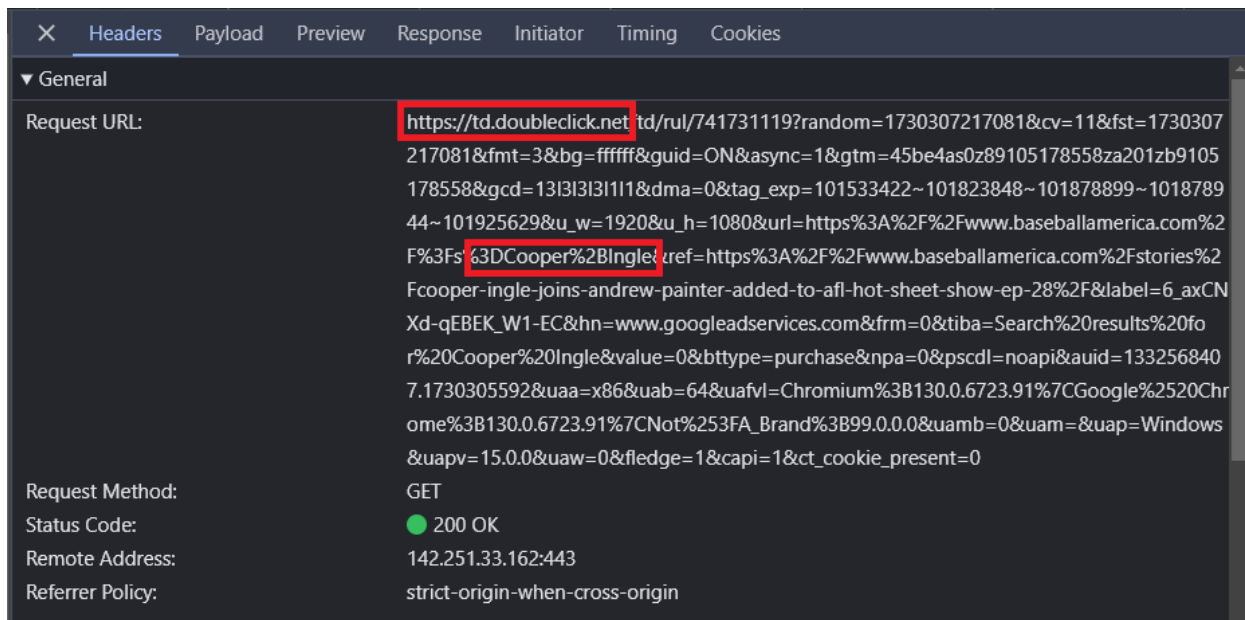


Figure 14 – Using Baseball America Website's Search Bar results in DoubleClick intercepting and obtaining search terms

⁷⁸ Joanna Geary, *DoubleClick (Google): What is it and what does it do?*, THE GUARDIAN (Apr. 23, 2012 12:08 PM), <https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring> (last visited Apr. 15, 2025).

146. The bidding system is similar to the Google Ads system. The benefits provided to Google from DoubleClick Ads are also similar to those provided by Google's search ads. First, Google Ad Manager has various fee structures that can be utilized including a percentage of spend plus a flat monthly fee; a flat monthly fee or percentage of spend, whichever is higher or a flat fee percentage based on the amount you spend every month.⁷⁹ Regardless of the structure, Google earns revenue from allowing website owners to utilize its code to display ads purchased from the DoubleClick Ad Exchange.

147. Google also aggregates data on what users are clicking on the website owner's sites to further improve their algorithms, develop their own products, and further drive revenue.⁸⁰

148. The Baseball America Website allows Google to integrate DoubleClick advertisements into its Website to further monetize its users. The website owner, here Defendant, receives money for selling the ad space on its Website, thus, directly benefitting from the DoubleClick implementation.

3. *Google Analytics*

149. Like the Facebook Pixel, Google Analytics ("GA") collects data about user interactions with a website, including: link clicks, button clicks, form submissions, conversions, shopping cart abandonment, adding items to carts, removing items from carts, file downloads,

⁷⁹ Joe Balestrino, *How Much Does Google Ads Management Cost?*, JOE BALESTRINO (Feb. 17, 2023), <https://www.joebalestrino.com/how-much-does-google-ads-management-cost> (last visited Apr. 15, 2025).

⁸⁰ Elle Poole Sidell, *What Does Google Do With Your Data?*, AVAST (Dec. 18, 2020), <https://www.avast.com/c-how-google-uses-your-data> (last visited Apr. 15, 2025).

scrolling behavior, video views, call to action performance, table of contents clicks, and other customizable events.⁸¹

150. The data collected through GA is sent back to Google, which associates the activity with the website it was collected from.⁸² Notably, Google notifies web developers that developers should provide “users with clear and comprehensive information about the data . . . collect[ed] on [their] websites” and to obtain “consent for that collection where legally required.”⁸³

151. In short, the use of GA represents specific data collection practices and settings and pre-determined destinations for that data. Google itself is aware of the potential legal violations its data collection tools are capable of, and puts the onus of warning users onto the website developers, such as Defendant.

152. Here, Defendant added GA to its Website, which resulted in the interception by and redirection of Plaintiffs’ search terms to Google, as depicted from the example taken directly from the Website below.

⁸¹ Zach Paruch, *What Is Google Tag Manager & How Does It Work?*, SEMRUSH BLOG (Jan. 4, 2024) <https://www.semrush.com/blog/beginners-guide-to-google-tag-manager/> (last visited Apr. 15, 2025).

⁸² *About the Google tag,* GOOGLE, <https://support.google.com/tagmanager/answer/11994839?hl=en> (last visited Apr. 15, 2025).

⁸³ *Id.*

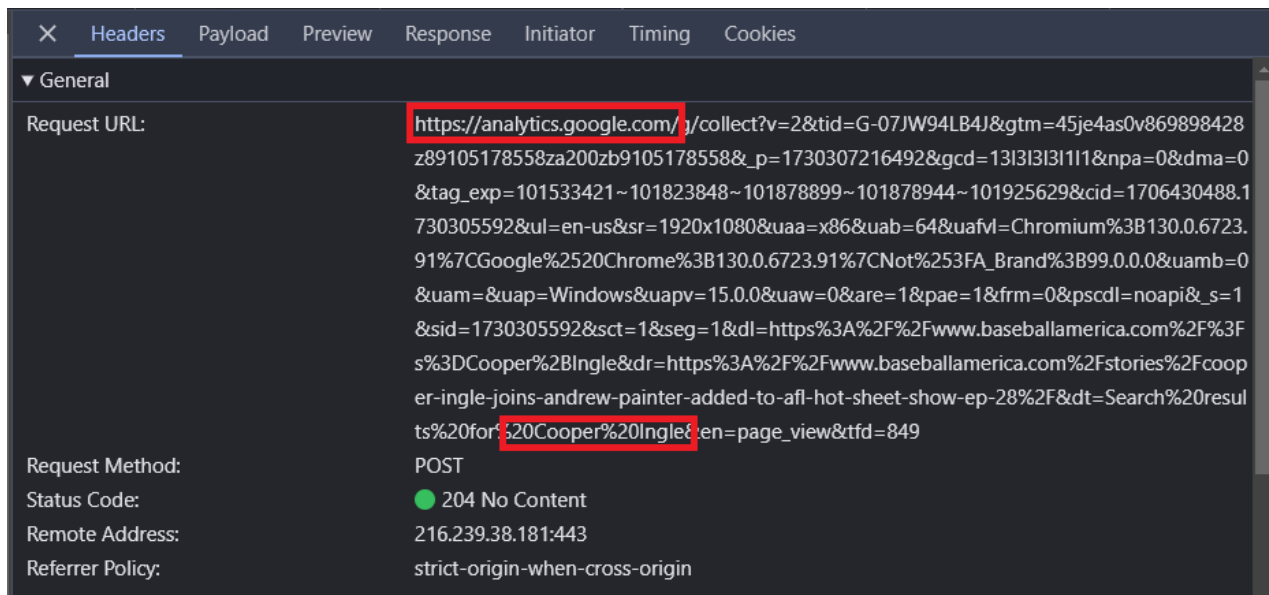


Figure 15 – Test search made on the Website resulted in sharing search terms with Google Analytics

153. After arriving at those common destinations, the Google products provide analysis and feedback which helps Defendant monetize the collected information through targeted advertising.

TOLLING

154. The statutes of limitations applicable to Plaintiffs' and the Classes' claims were tolled by Defendant's conduct and Plaintiffs' and Class Members' delayed discovery of their claims.

155. As alleged above, Plaintiffs and members of the Classes did not know and could not have known when they used the Website that Defendant was disclosing their information and communications to third parties. Plaintiffs and members of the Classes could not have discovered Defendant's unlawful conduct with reasonable diligence.

156. Defendant secretly incorporated the Pixel into the Website, providing no indication to Subscribers that their communications would be disclosed to Facebook.

157. Defendant had exclusive and superior knowledge that Facebook's Pixel incorporated on its Website would disclose Subscribers' protected and private information and confidential communications yet failed to disclose that by interacting with the Website, Plaintiffs' and Class Members' Sensitive Information would be disclosed to Facebook.

158. Plaintiffs and members of the Classes could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Facebook's Pixel is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Website Subscriber that Defendant was disclosing and allowing the interception of such information Facebook.

159. The earliest Plaintiffs and Class Members could have known about Defendant's conduct was in connection with their investigation and the work done on their behalf in preparation of filing of this Complaint.

CLASS ACTION ALLEGATIONS

160. Plaintiffs bring this action individually and on behalf of the following Classes:

All persons in the United States with a subscription to the Website who had their Sensitive Information improperly disclosed to third parties through the use of the Tracking Tools (the "Class").

All persons in Pennsylvania with a subscription to the Website who had their Sensitive Information improperly disclosed to third parties through the use of the Tracking Tools (the "Pennsylvania Subclass").

161. Specifically excluded from the Classes are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

162. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Classes should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

163. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

164. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Classes. However, given the popularity of Defendant's Website, the number of persons within the Classes is believed to be so numerous that joinder of all members is impractical.

165. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Classes because Plaintiffs, like all members of the Classes, subscribed to, and used, the Website to watch videos, and had their Sensitive Information collected and disclosed by Defendant.

166. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have no interests antagonistic to, nor in conflict with, the Classes. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

167. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

168. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Classes that predominate over questions that may affect individual members of the Classes include:

- a. Whether Defendant collected Plaintiffs' and the Classes' Sensitive Information;
- b. Whether Defendant unlawfully disclosed and continues to disclose the Sensitive Information of Subscribers of the Website in violation of the VPPA, the Wiretap Act, and WESCA;
- c. Whether Defendant's disclosures were committed knowingly; and
- d. Whether Defendant disclosed Plaintiffs' and the Classes' Sensitive Information without consent.

169. Information concerning Defendant's Website's data sharing practices and account members is available from Defendant's or third-party records.

170. Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

171. The prosecution of separate actions by individual members of the Classes would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

172. Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Classes as a whole.

173. Given that Defendant's conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I

**VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, *et seq.*
(On Behalf of Plaintiffs and the Class)**

174. Plaintiffs hereby incorporate by reference and re-allege herein the allegations contained in all preceding paragraphs of this complaint.

175. Plaintiffs bring this count on behalf of themselves and all members of the Class.

176. The VPPA provides that “a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d).” 18 U.S.C. § 2710(b)(1).

177. “Personally-identifiable information” is defined to include “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3).

178. A “video tape service provider” is “any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

179. Defendant violated this statute by knowingly disclosing Plaintiffs’ and other Class Members’ personally identifiable information to Facebook.

180. Defendant, through the Website, engages in the business of delivering video content to Subscribers, including Plaintiffs and the other Class Members, and other users. The Website delivers videos to Subscribers, including Plaintiffs and the other Class Members, by making those materials available to Plaintiffs and the other Class Members on the Website.

181. Defendant is a “video tape service provider” because it curates, hosts, provides access to, and causes the delivery of thousands of videos on the Website, thereby “engag[ing] in

the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

182. Defendant solicits individuals to pay to subscribe to the Website.

183. Plaintiffs and members of the Class are “consumers” because they paid to subscribe to Defendant’s Website. 18 U.S.C. § 2710(a)(1).

184. Plaintiffs and members of the Class viewed videos on the Website.

185. Defendant disclosed Plaintiffs’ and Class Members’ personally identifiable information to Facebook. Defendant utilized the Pixel which forced Plaintiffs’ web browser to transmit Plaintiffs’ identifying information, like her Facebook ID, along with Plaintiffs’ and Class Members’ event data, including the title of the videos they viewed, to Facebook.

186. Defendant knowingly disclosed Plaintiffs’ and Class Members’ PII, which is triggered automatically through Defendant’s use of the Pixel. No additional steps on the part of Defendant, Facebook, or any third party are required. Once the Pixel’s routine exchange of information is complete, the UID that becomes available can be used by any individual to easily identify a Facebook user. *See* Section B(2) (process to identify an individual using a UID).

187. Plaintiffs and members of the Class did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to Facebook. Defendant failed to obtain “informed, written consent” from consumers – including Plaintiffs and members of the Class – “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer” and “at the election of the consumer,” either “given at the time the disclosure is sought” or “given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner.” 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

188. Defendant’s disclosures of Plaintiffs’ and Class Members’ PII were not made in the “ordinary course of business” as the term is defined by the VPPA. In particular, Defendant’s

disclosures to Facebook were not necessary for “debt collection activities, order fulfillment, request processing, [or] transfer of ownership.” 18 U.S.C. § 2710(a)(2). Instead, Plaintiffs’ and Class Members’ PII was used for improving marketing effectiveness.

189. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also “provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer’s election.” Defendant failed to provide an opportunity to opt-out as required by the VPPA.

190. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief as to Defendant; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with VPPA’s requirements for protecting a consumer’s PII; (iii) statutory damages of \$2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c); and (iv) reasonable attorneys’ fees and costs and other litigation expenses.

Injunctive Relief Of Defendant’s Ongoing VPPA Violations

191. An actual and immediate controversy has arisen and now exists between Plaintiffs and the putative class she seeks to represent, and Defendant, which parties have a genuine and opposing interest in and which their interests are direct and substantial. Defendant has violated, and continues to violate, Plaintiffs’ and Class Members’ rights to protect their PII under the VPPA.

192. Plaintiffs have demonstrated that they are likely to succeed on the merits of their claims, and are thus entitled to declaratory and injunctive relief.

193. Plaintiffs have no adequate remedy at law to stop the continuing violations of the VPPA by Defendant. Unless enjoined by the Court, Defendant will continue to infringe on the privacy rights of Plaintiffs, Class Members, and the absent Class Members, and will continue to

cause, or allow to be caused, irreparable harm to Plaintiffs and Class Members. Injunctive relief is in the public interest to protect the PII of Plaintiffs and Class Members, and other consumers that would be irreparably harmed through continued disclosure of their PII.

194. Defendant completely disregards its obligation under the VPPA by loading the Pixel onto the Website and facilitating the sharing of consumers' PII with Facebook for any ordinary person to access and use.

195. Despite brazenly violating the VPPA, consumers were provided with no notice of the employment of the Pixel and no indication of how or how much of their information was shared with Facebook. Worse, in further violation of the VPPA, Defendant did not seek or obtain any form of consent from subscribers for the use of the Pixel to share information improperly pulled from the Website.

196. This threat of injury to Plaintiffs and members of the Class from the continuous violations requires temporary, preliminary, and permanent injunctive relief to ensure their PII is protected from future disclosure.

COUNT II

VIOLATION OF THE FEDERAL WIRETAP ACT 18 U.S.C. § 2510, *et seq.* (On Behalf of Plaintiffs and the Class)

197. Plaintiffs hereby incorporate by reference and re-allege herein the allegations contained in all preceding paragraphs of this Complaint.

198. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

199. Codified under 18 U.S.C. §§ 2510 *et seq.*, the Federal Wiretap Act (the "Wiretap Act") prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

200. The Wiretap Act confers a civil private right of action to “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.” 18 U.S.C. § 2520(a).

201. The Wiretap Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

202. The Wiretap Act defines “contents” as “includ[ing] any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

203. The Wiretap Act defines person as “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

204. The Wiretap Act defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce” 18 U.S.C. § 2510(12).

205. Defendant is a person for purposes of the Wiretap Act.

206. The Pixel constitutes a “device or apparatus which can be used to intercept a wire, oral, or electronic communication.” 18 U.S.C. § 2510(5).

207. The confidential communications Plaintiffs and members of the Class had with the Website, in the form of their browsing information, were intercepted by Facebook and such communications were “electronic communications” under 18 U.S.C. § 2510(12).

208. Plaintiffs and members of the Class had a reasonable expectation of privacy in their electronic communications with the Website in the form of their browsing information. Even if Plaintiffs and members of the Class had no reasonable expectation of privacy in the electronic communications, Plaintiffs’ and Class Members’ electronic communications with the Website included descriptions and summaries of the pre-recorded video content they viewed along with their PII, giving rise to a reasonable expectation of privacy under the VPPA.

209. Plaintiffs and members of the Class reasonably expected that third parties were not intercepting, recording, or disclosing their electronic communications with the Website.

210. Within the relevant time period, the electronic communications between Plaintiffs and members of the Class and the Website were intercepted during their transmission, without consent, and for the unlawful and wrongful purpose of monetizing their private information, which includes the purpose of using such private information to develop advertising and marketing strategies.

211. Interception of Plaintiffs' and Class Members' confidential communications with the Website occurs whenever a user navigates various web pages of the Website.

212. At all times relevant to this Complaint, Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge regarding the functionality of the Pixel, including that allowing the Pixel to be implemented on the Website would cause the communications of their users to be shared with Facebook.

213. Plaintiffs and members of the Class were never asked for their consent to share their confidential electronic communications with the Website with Facebook. Indeed, such consent could not have been given as none of Facebook, Defendant or the Website ever sought any form of consent from Plaintiffs or members of Class to intercept, record, and disclose their private communications with the Website.

214. As detailed above, Facebook's unauthorized interception, disclosure, and use of Plaintiffs' and the Class Members' confidential communications was only possible through Defendant's knowing, willful, or intentional placement of the Pixel on the Website. 18 U.S.C. § 2511(1)(a).

215. Plaintiffs and members of the Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs and members of the Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and members of the Class and any profits made by Facebook as a result of the violation,

or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$10,000; and (2) appropriate equitable or declaratory relief; (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT III

VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT ("WESCA")

18 Pa. C.S.A. § 5701, *et seq.*

(On Behalf of Plaintiff Messina and the Pennsylvania Subclass)

1. Plaintiff Messina incorporates by reference and re-alleges each and every allegation set forth in all preceding paragraphs of this Complaint.

2. Plaintiff Messina brings this claim individually and on behalf of the members of the proposed Pennsylvania Subclass against Defendant.

3. Defendant is a "person" as defined by 18 Pa. C.S.A. § 5702.

4. WESCA prohibits any person from willfully intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication. 18 Pa. C.S.A. §§ 5701, 5703(1).

5. Defendant procured the Tracking Entities' services to "intercept" Plaintiff Messina's and Pennsylvania Subclass Members' communications with Baseball America, pursuant to WESCA, which defines "intercept" as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

6. Baseball America subsequently used the contents of Plaintiff Messina's communications with Baseball America, intercepted and processed by the Tracking Entities, to target users with advertising, which is prohibited under WESCA. 18 Pa. C.S.A. § 5703(2)-(3).

7. WESCA also prohibits the knowing access to obtain access to a wire or electronic communication while it is in electronic storage by intentionally accessing, or exceeding the scope

of access to, a facility through which an electronic communication service is provided. 18 Pa. C.S.A. § 5741(a)(1)-(2).

8. Baseball America obtained Tracking Tools from the Tracking Entities to intercept and/or improperly access the communications between Baseball America and its Subscribers in the conduct of its business, in violation of WESCA.

9. The devices used in this case, include, but are not limited to:

- a. Baseball America's own computers, which were used to add the Pixel to its web pages;
- b. Baseball America's servers used to host its web pages;
- c. Plaintiff Messina's and Pennsylvania Subclass Members' personal computing devices;
- d. Plaintiff Messina's and Pennsylvania Subclass Members' web browsers;
- e. The Pixel itself;
- f. Internet cookies;
- g. Third-party code utilized by Baseball America; and
- h. Computer servers of third parties (including the Tracking Entities).

10. Defendant aided in the interception of communications between Plaintiff Messina and Pennsylvania Subclass Members and Defendant that were subsequently redirected to and recorded by third parties without Plaintiff Messina's or Pennsylvania Subclass Members' consent.

11. WESCA confers a private civil cause of action to any person whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a).

12. Plaintiff Messina and the Pennsylvania Subclass Members are Subscribers of Defendant's Website. Because Plaintiff Messina and Pennsylvania Subclass Members plan to continue to use Defendant's Website in the future, if Defendant's unfair, unlawful, and deceptive trade practices are allowed to continue, Plaintiff Messina and Pennsylvania Subclass Members are likely to suffer continuing harm in the future.

13. Defendant's WESCA violation was highly offensive enough to cause mental suffering because Defendant was entrusted with personal and private information – information that is protected by federal and state law – and disclosed that information to third parties. *See Doe v. Redeemer Health*, 2023 Phila. Ct. Com.Pl. LEXIS 17, at *1 fn. 2 (Phila. Ct. Com. Pl. Sept. 16, 2024).

14. Plaintiff Messina and members of the Pennsylvania Subclass seek all relief available for violations of WESCA, including recovery of actual damages that are not less than liquidated damages computed at a rate of \$100.00 a day for each day of violation or \$1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred, along with injunctive relief.

COUNT IV

INTRUSION UPON SECLUSION (On Behalf of Plaintiffs and the Class)

216. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in all preceding paragraphs of this Complaint.

217. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

218. Defendant intentionally intruded upon Plaintiffs' and Class Members' solitude or seclusion in that it effectively placed Facebook in the middle of conversations including Sensitive Information to which it was not an authorized party.

219. Defendant's participation in Facebook's tracking and interception of Sensitive Information was not authorized by Plaintiffs or Class Members.

220. Defendant's enabling of Facebook's intentional intrusion into Plaintiffs' and Class Members' internet communications including PII and their computing devices and web browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individuals' privacy and against theft.

221. Secret monitoring of Sensitive Information is highly offensive behavior.

222. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is handling PII. Plaintiffs and Class Members have been damaged by Defendant's facilitation of Facebook's intrusion upon their seclusion and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representative of the Class and their counsel as Class Counsel;
- (b) For an order declaring that Defendant's conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;
- (d) For entry of an order for injunctive and declaratory relief as described herein, including, but not limited to requiring Defendant to immediately (i) remove the Pixel from the Website or (ii) add, and obtain, the appropriate consent from Subscribers;
- (e) For damages in amounts to be determined by the Court and/or jury;
- (f) For an award of statutory damages or penalties to the extent available;
- (g) For Defendant to pay \$2,500.00 to Plaintiffs and members of the Class, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);
- (h) For pre-judgment interest on all amounts awarded;
- (i) For an order of restitution and all other forms of monetary relief;
- (j) An award of all reasonable attorneys' fees and costs; and
- (k) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: April 22, 2025

By: s/ David M. Wilkerson

N.C. Bar No. 35742

Wilkerson Justus PLLC

P.O. Box 54

Asheville, NC 28802

(828) 316-6902

dwilkerson@wilkersonjustus.com

Mark S. Reich*

Gary S. Ishimoto*

LEVI & KORSINSKY, LLP

33 Whitehall Street, 17th Floor

New York, NY 10004

Telephone: (212) 363-7500

Facsimile: (212) 363-7171

Email: mreich@zlk.com

Email: gishimoto@zlk.com

Counsel for Plaintiffs

**pro hac vice forthcoming*